AMENDMENTS TO THE SPECIFICATION

Please amend paragraph [0071] as follows:

[0071] In block 220, a client sends a certificate signed by a CA to a server. For example, a client 101 sends a certificate to a server 110 that has been signed by a certificate authority 120. In alternative embodiments, the client's certificate is not ~~be~~ signed by a CA.

Please amend paragraph [0082] as follows;

[0082] In block 335, a client and a server engage in a security handshake. Here a server sends a message encrypted with its private key to the client. The client then decrypts the message with the server's public key in order to validate that the server holds the private key. An example of such a security handshake is the Secure Socket Layer (SSL) handshake performed as part of the SSL protocol. For example, a client 101 that has opened an https connection with a server 110 performs a SSL handshake as part of its connection protocol. In doing so, the server 110, would send and encrypted message (using its private key) to a client 101. The client 101 would then decrypt the message using the server's 110 ~~private~~ public key. In alternative embodiments, this secure handshake step is omitted.

Please amend paragraph [0092] as follows:

[0092] In block 420, the certificate on the server, if one exists, it is replaced with the new certificate obtained form the CA. For example, a server 110 replaces its certificate with a new one that it has obtained ~~form~~ from a CA 120.

Please amend paragraph [0095] as follows;

[0095] There are many reasons that a certificate could be revoked for a ~~server~~ client, including, expiration of the certificate, change of certificate authority, and compromise of the certificate. In any of these cases, the certificate needs to be replaced, as do the copies of the certificate resident on the clients.

Please amend the section heading at the bottom page 12 following paragraph [0101] as follows:

COMPARING MEMORY ~~REPEESNTATIONS~~ REPRESENTATIONS